(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－95984

(43)公開日　平成11年(1999)４月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	7/58		Ｇ０６Ｆ	7/58	Ｃ
Ｇ０９Ｃ	1/00	６５０	Ｇ０９Ｃ	1/00	６５０Ｂ

審査請求　有　　請求項の数14　ＦＤ　（全 15 頁）

(21)出願番号　特願平9－276517

(22)出願日　平成９年(1997)９月24日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　島田　道雄
東京都港区芝五丁目７番１号　日本電気株式会社内

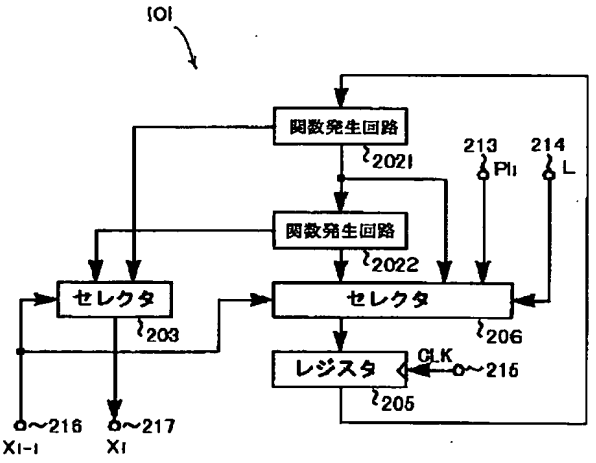
(74)代理人　弁理士　野田　茂

(54)【発明の名称】　擬似乱数発生方法および装置

(57)【要約】

【課題】　暗号学的に安全性の高い擬似乱数を容易に発生できるようにする。

【解決手段】　擬似乱数発生回路１０１のレジスタ２０５は、複数のビットから成る状態データを、クロック信号ＣＬＫの各クロックパルスに同期して取り込んで保持し、関数発生回路２０２１、２０２２はレジスタ２０５が保持している状態データに応じてそれぞれ複数のビットから成るデータを出力する。そしてセレクタ２０３は上記関数発生回路がそれぞれ出力する２つのデータのうちのいずれかのデータの特定のビットを、前段の擬似乱数発生回路が発生した擬似乱数X_{i-1}にもとづいて選択し擬似乱数X_iとして出力する。一方、セレクタ２０６は上記関数発生回路がそれぞれ出力するデータのうちのいずれかのデータの、上記特定のビットを除いたデータを、前段の擬似乱数発生回路が発生した擬似乱数X_{i-1}にもとづいて選択しレジスタ２０５に状態データとして供給する。



1

【特許請求の範囲】

【請求項１】　順序づけられた複数の擬似乱数発生回路を用い、前段の前記擬似乱数発生回路が発生した第１の擬似乱数にもとづいて各擬似乱数発生回路に第１の擬似乱数を発生させ、前記複数の擬似乱数発生回路が発生した前記第１の擬似乱数により第２の擬似乱数を発生する擬似乱数発生方法において、

各擬似乱数発生回路では、

複数のビットから成る状態データを保持し、

保持した前記状態データに応じて複数のビットから成る第１および第２のデータを発生し、

前記第１および第２のデータのうちのいずれかのデータの特定のビットを、前段の前記擬似乱数発生回路が発生した前記第１の擬似乱数にもとづいて選択し前記第１の擬似乱数として出力し、

前記第１および第２のデータのうちのいずれかのデータの、前記特定のビットを除いたデータを、前段の前記擬似乱数発生回路が発生した前記第１の擬似乱数にもとづいて選択し次に保持すべき前記状態データとする、

ことを特徴とする擬似乱数発生方法。

【請求項２】　保持した前記状態データに応じて複数のビットから成る順序づけられた複数のデータを発生し、

前記複数のデータのうちの１番目のデータは保持した前記状態データから直接発生し、２番目以降のデータはそれぞれ１つ前のデータから発生し、

前記第１のデータは前記複数のデータのうちの最後のデータを除くいずれかのデータであり、

前記第２のデータは前記複数のデータのうちの最後のデータである、

ことを特徴とする請求項１記載の擬似乱数発生方法。

【請求項３】　S_0、S_1を$0<S_0<S_1$を満たす整数として前記第１のデータは前記複数のデータのうちのS_0番目のデータであって前記第２のデータはS_1番目の前記データであり、

ｉを１以上の整数としてｉ番目の前記擬似乱数発生回路が発生する前記第１の擬似乱数の系列の周期をL_iとし、

ｉ番目の前記擬似乱数発生回路が発生する前記第１の擬似乱数の系列の１周期中に出現する論理”１”の数をW_iとし、

任意のｉに対してL_iと$(L_{i-1}-W_{i-1})\times S_0+W_{i-1}\times S_1$とが互いに素で、２より大きい任意のｉに対して$L_i$と$L_1\times L_2\times\cdots\times L_{i-2}$とが互いに素である、

ことを特徴とする請求項２記載の擬似乱数発生方法。

【請求項４】　前記複数の擬似乱数発生回路により発生した前記第１の擬似乱数の排他的論理和を算出し、算出結果を前記第２の擬似乱数とすることを特徴とする請求項１記載の擬似乱数発生方法。

【請求項５】　前記複数の擬似乱数発生回路のそれぞれに対応させて排他的論理和回路を設け、

2

各排他的論理和回路には、対応する前記擬似乱数発生回路が発生した前記第１の擬似乱数と、前段の前記擬似乱数発生回路に対応する前記排他的論理和回路が算出した擬似乱数との排他的論理和を算出させ、

最後の前記擬似乱数発生回路に対応する前記排他的論理和回路に算出させた擬似乱数を前記第２の擬似乱数とする、

ことを特徴とする請求項１記載の擬似乱数発生方法。

【請求項６】　前記特定のビットは１つまたは複数のビットから成ることを特徴とする請求項１記載の擬似乱数発生方法。

【請求項７】　前記擬似乱数発生回路は非線型擬似乱数発生回路であることを特徴とする請求項１記載の擬似乱数発生方法。

【請求項８】　順序づけられた複数の擬似乱数発生回路を備え、各擬似乱数発生回路は前段の前記擬似乱数発生回路が発生した第１の擬似乱数にもとづいて第１の擬似乱数を発生し、前記複数の前記擬似乱数発生回路が発生した前記第１の擬似乱数により第２の擬似乱数を発生する擬似乱数発生装置において、

各擬似乱数発生回路は、

複数のビットから成る状態データを、クロック信号の各クロックパルスに同期して取り込んで保持するレジスタと、

前記レジスタが保持している前記状態データに応じて複数のビットから成る第１および第２のデータをそれぞれ出力する第１および第２の関数発生回路と、

前記第１および第２の関数発生回路がそれぞれ出力する前記第１および第２のデータのうちのいずれかのデータの特定のビットを、前段の前記擬似乱数発生回路が発生した前記第１の擬似乱数にもとづいて選択し前記第１の擬似乱数として出力する第１のセレクタと、

前記第１および第２の関数発生回路がそれぞれ出力する前記第１および第２のデータのうちのいずれかの前記データの、前記特定のビットを除いたデータを、前段の前記擬似乱数発生回路が発生した前記第１の擬似乱数にもとづいて選択し前記レジスタに前記状態データとして供給する第２のセレクタと、

を備えたことを特徴とする擬似乱数発生装置。

【請求項９】　前記レジスタが保持している状態データに応じて複数のビットから成るデータをそれぞれ出力する順序づけられた複数の関数発生回路を含み、

１番目の前記関数発生回路は前記レジスタが保持している前記状態データに直接したがって前記データを出力し、２番目以降の前記関数発生回路はそれぞれ１つ前の前記関数発生回路が出力したデータにしたがって前記データを出力し、

前記第１の関数発生回路は前記複数の関数発生回路のうちの最後の関数発生回路を除くいずれかの関数発生回路であり、

第２の前記関数発生回路は前記複数の関数発生回路のうちの最後の関数発生回路である、
ことを特徴とする請求項８記載の擬似乱数発生装置。
【請求項１０】　S_0、S_1を$0<S_0<S_1$を満たす整数として前記第１の関数発生回路は前記複数の関数発生回路のうちのS_0番目の関数発生回路であって前記第２の関数発生回路はS_1番目の関数発生回路であり、
ｉを１以上の整数としてｉ番目の前記擬似乱数発生回路が発生する前記第１の擬似乱数の系列の周期をL_iとし、
ｉ番目の前記擬似乱数発生回路が発生する前記第１の擬似乱数の系列の１周期中に出現する論理”１”の数をW_iとし、
任意のｉに対してL_iと$(L_{i-1}-W_{i-1})\times S_0+W_{i-1}\times S_1$とが互いに素で、２より大きい任意のｉに対して$L_i$と$L_1\times L_2\times\cdots\times L_{i-2}$とが互いに素である、
ことを特徴とする請求項９記載の擬似乱数発生装置。
【請求項１１】　前記複数の擬似乱数発生回路がそれぞれ発生した前記第１の擬似乱数の排他的論理和を算出して前記第２の擬似乱数として出力する排他的論理和回路を備えたことを特徴とする請求項８記載の擬似乱数発生装置。
【請求項１２】　前記複数の擬似乱数発生回路のそれぞれに対応する排他的論理和回路を有し、
各擬似乱数発生回路に対応する前記排他的論理和回路の一方の入力端子には対応する前記擬似乱数発生回路が発生した前記第１の擬似乱数が供給され、もう一方の入力端子は前段の前記擬似乱数発生回路に対応する排他的論理和回路の出力端子に接続され、
最後の前記擬似乱数発生回路に対応する前記排他的論理和回路から前記第２の擬似乱数が出力される、
ことを特徴とする請求項８記載の擬似乱数発生装置。
【請求項１３】　前記特定のビットは１つまたは複数のビットから成ることを特徴とする請求項８記載の擬似乱数発生装置。
【請求項１４】　前記擬似乱数発生回路は非線型擬似乱数発生回路であることを特徴とする請求項８記載の擬似乱数発生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は擬似乱数の発生方法および装置に関するものである。
【０００２】
【従来の技術】１つの擬似乱数発生回路に供給されるクロック信号を別の擬似乱数発生回路の出力する擬似乱数に依存して操作することは古くから行われており、第２次世界大戦中の機械式暗号にまで起源を遡ることができる。また、日本軍の暗号の専門家であった加藤正隆が著した「基礎暗号学」（１９８９年サイエンス社発行）にも、Ｍ系列発生器の出力を間引くことによって良質な擬似乱数を発生できることが記述されている。しかしながら、クロック信号を操作する擬似乱数発生装置には理論的な解析が難しいという問題があった。
【０００３】このため、理論的に評価されているのは、後述の「段数の等しい線形フィードバック・シフトレジスタ（ＬＦＳＲ）」（特にＭ系列発生器と呼ばれるＬＦＳＲ）をカスケード接続した擬似乱数発生装置（図７）に限られていた。しかしながら、このような従来の擬似乱数発生装置には、ロックインの問題があり、ロックインを利用した暗号解読を防ぐために、多数のＬＦＳＲをカスケード接続しなければならないという欠点があった。
【０００４】ロックインの問題とは、初段のＬＦＳＲが出力する擬似乱数にもとづいて発生されたクロック制御信号によっては、連続する複数のクロックの期間にわたって次段のＬＦＳＲにクロックが供給されなくなる場合があり、その際、残りのＬＦＳＲも動作を停止してしまい、擬似乱数発生装置が出力する擬似乱数がこの期間中同じ値をとってしまうという問題である。なお、この問題および関連する事柄については、例えば、ゴールマンとチャンバーズの著した論文「クロック・コントロールド・シフトレジスターズ：ア・レビュー」（Ｄｉｅｔｅｒ Ｇｏｌｌｍａｎｎ ａｎｄ Ｗｉｌｌｉａｍ Ｇ. Ｃｈａｍｂｅｒｓ、”Ｃｌｏｃｋ－ＣｏｎｔｒｏｌｌｅｄＳｈｉｆｔ Ｒｅｇｉｓｔｅｒｓ：Ａ Ｒｅｖｉｅｗ”、ＩＥＥＥ Ｊｏｏｕｒｎａｌ ｏｎＳｅｌｅｃｔｅｄ Ａｒｅａｓ ｉｎ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ、Ｖｏｌ．７、Ｎｏ．４、ｐｐ．５２５－５３３、Ｍａｙ １９８９）や、シュナイアによる「アプライド・クリプトグラフィー」（Ｂｒｕｃｅ Ｓｃｈｎｅｉｅｒ、Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ：Ｐｒｏｔｏｃｏｌｓ、Ａｌｇｏｒｉｔｈｍｓ、ａｎｄ Ｓｏｕｒｃｅ Ｃｏｄｅ ｉｎ Ｃ、２ｎｄ Ｅｄｉｔｉｏｎ、Ｊｏｈｎ Ｗｉｌｅｙ ＆ Ｓｏｎｓ、１９９６）などの書籍に詳しく解説されている。
【０００５】図７は、擬似乱数発生回路として線形フィードバック・シフトレジスタ（ＬＦＳＲ）をカスケード接続した従来の擬似乱数発生装置の基本構成を示す機能ブロック図である。図に示したように、この擬似乱数発生装置は順番に配列されたｎ（ｎは正の整数）のＬＦＳＲ９０２を備え、各ＬＦＳＲ９０２はそれぞれｍビット（ｍは正の整数）の内部状態を持っている。そして、ｉ番目（ｉは正の整数）のＬＦＳＲ９０２は、入力端子１０４に供給されている制御信号Ｌの値が論理”０”の時には、ｉ番目の論理和回路９０１からクロック信号が供給されたら、入力端子１０５から供給されるｎ×ｍビットのビット列のうちｍビットのビット列を取り込んで内部状態として保持し、一方、入力端子１０４に供給されている制御信号Ｌが論理”１”の時には、上記論理和回

路９０１からクロック信号が供給されるごとに、内部状態を１クロックパルス分だけ進めるとともに、発生した擬似乱数X_i（１ビット）を出力する。

【０００６】ｉ番目の排他的論理和回路８０２は、擬似乱数X_iと、ｉ－１番目の排他的論理和回路８０２が出力する擬似乱数Y_{i-1}との排他的論理和を計算し、計算結果として得られる擬似乱数Y_iを、クロック制御信号としてｉ＋１番目のＬＦＳＲ９０２に供給すると共にｉ＋１番目の排他的論理和回路８０２に供給する。なお、最後の排他的論理和回路８０２は、排他的論理和の計算結果として得られる擬似乱数Y_nをこの擬似乱数発生装置の出力として出力端子１０６より出力する。

【０００７】ｉ番目の論理和回路９０１は、入力端子１０３から供給されるクロック信号ＣＬＫとクロック制御信号Y_{i-1}との論理和を計算して計算結果を出力するので、クロック制御信号Y_{i-1}の論理値が論理”０”であれば、論理和回路９０１は入力端子１０３から供給されたクロック信号をそのまま出力するが、クロック制御信号Y_{i-1}が論理”１”であれば、入力端子１０３から供給されたクロック信号はこの論理和回路９０１で阻止される。そのため、クロック制御信号Y_{i-1}が論理”０”の時には、入力端子１０３からクロック信号が供給されると、ｉ番目のＬＦＳＲ９０２の内部状態が更新されるが、クロック制御信号Y_{i-1}が論理”１”の時には、入力端子１０３からクロック信号が供給されても、このＬＦＳＲ９０２の内部状態は更新されない。なお、クロック制御信号Y_0は予め決められた定数であり、例えばY_0＝０とする。

【０００８】ここで図７の擬似乱数発生装置などを構成するために用いる従来の擬似乱数発生回路について詳しく説明しておく。図８は従来の基本的な構成の擬似乱数発生回路の一例を示す機能ブロック図である。図において、レジスタ２０５は、入力端子３１５からクロック信号ＣＬＫが供給されると、セレクタ２０４が出力するｍビットのデータを内部状態を表すデータとして保持し、同時に保持したデータを関数発生回路２０２に供給する。関数発生回路２０２は、レジスタ２０５から供給されるｍビットのデータに対して予め決められた変換を施し、１ビットを加えて合計ｍ＋１ビットのデータを発生する。そして、このデータのｍ＋１ビットのうちのｍビットをセレクタ２０４に供給し、一方、残りの１ビットは擬似乱数として出力端子３１７から出力する。

【０００９】セレクタ２０４は、入力端子３１４に供給されている制御信号Ｌが論理”０”の時には、入力端子３１３に供給されているｍビットのデータを選択して出力し、一方、入力端子３１４に供給されている制御信号Ｌが論理”１”の時には、関数発生回路２０２が出力するｍビットのデータを選択して出力する。この擬似乱数発生回路では、関数発生回路２０２はレジスタ２０５の現在の内部状態を表すデータを変換して出力し、レジスタ２０５は、通常の動作状態においてクロック信号ＣＬＫの各クロックパルスが入力されるごとに、セレクタ２０４を通じて関数発生回路２０２が出力するデータを取り込んで保持する。したがって、各クロックパルスが入力されるごとに内部状態が変化し、変化した内部状態にもとづいて関数発生回路２０２は擬似乱数を発生して端子３１７から出力する。

【００１０】図９は、特に非線形フィードバック・シフトレジスタと呼ばれる従来の擬似乱数発生回路の基本構成を示す機能ブロック図である。図中、図８と同一の要素には同一の符号が付されており、それらに関する説明はここでは省略する。この擬似乱数発生回路は、関数発生回路２０２の構成において上述した擬似乱数発生回路と異なっている。すなわちこの擬似乱数発生回路では、関数発生回路２０２は関数発生回路４０１およびシフタ４０２により構成されている。関数発生回路４０１は、ｍビットの入力データに対して１ビットのデータを出力するものであり、出力データはシフタ４０２に供給すると共に、出力端子３１７を通じて擬似乱数として出力する。シフタ４０２は、レジスタ２０５から供給されるｍビットのデータを右に１ビットシフトさせて左側のｍ－１ビットを取り出し、さらに、最左端に関数発生回路４０１からの１ビットの出力データを付加してｍビットのデータとした上でセレクタ２０４を通じてレジスタ２０５に供給する。

【００１１】したがってこの擬似乱数発生回路でも、関数発生回路２０２はレジスタ２０５の現在の内部状態を表すデータを、関数発生回路４０１およびシフタ４０２の作用によって変換して出力し、レジスタ２０５は、通常の動作状態においてクロック信号ＣＬＫの各クロックパルスが入力されるごとに、セレクタ２０４を通じて関数発生回路２０２が出力するデータを取り込んで保持する。したがって、各クロックパルスが入力されるごとに内部状態が変化し、変化した内部状態にもとづいて関数発生回路２０２は擬似乱数を発生して端子３１７から出力する。

【００１２】図１０は、図７の擬似乱数発生装置を構成する線形フィードバック・シフトレジスタの基本構成を示す機能ブロック図である。図中、図８、図９と同一の要素には同一の符号が付されており、それらに関する説明はここでは省略する。図１０に示したＬＦＳＲ９０２は、関数発生回路４０１が排他的論理和回路５０１により構成されている点で図９の擬似乱数発生回路と異なっている。排他的論理和回路５０１は、レジスタ２０５からのデータを構成するｍビットのうち予め決められた複数ビットの排他的論理和を算出し、結果を出力端子３１７に出力すると共に、シフタ４０２に供給する。

【００１３】したがって、このＬＦＳＲ９０２でも、関数発生回路２０２はレジスタ２０５からの現在の内部状態を表すデータを変換して出力し、レジスタ２０５は、

通常の動作状態においてクロック信号ＣＬＫの各クロックパルスが入力されるごとに、セレクタ２０４を通じて関数発生回路２０２が出力するデータを取り込んで保持する。したがって、各クロックが入力されるごとに内部状態が変化し、変化した内部状態にもとづいて関数発生回路２０２は擬似乱数を発生し、端子３１７から出力する。このようなＬＦＳＲ９０２で、発生される擬似乱数の周期が2^m-1である場合には、このＬＦＳＲは特にＭ系列発生器と呼ばれる。

【００１４】

【発明が解決しようとする課題】しかし、図７に示した従来の擬似乱数発生装置では、入力端子１０３からクロック信号が入力されても、クロック制御信号Y_{i-1}が論理”１”の時には、上記クロックは論理和回路９０１で阻止され、したがって、ＬＦＳＲ９０２の内部状態は更新されない。その結果、上述したロックインの問題が発生し、ロックインを利用した暗号解読を防ぐべく、多数のＬＦＳＲ９０２をカスケード接続しなければならなくなる。そのため、従来の擬似乱数発生装置は規模が大きく、かつコスト高となっていた。また、装置の規模およびコストに配慮して設計した場合には、性能が抑えられる結果となっていた。

【００１５】そこで本発明の目的は、ロックインの問題を解決して小規模、低コストで、かつ暗号学的な安全性の高い擬似乱数を発生できる擬似乱数発生方法および装置を提供することにある。

【００１６】

【課題を解決するための手段】本発明は上記目的を達成するため、順序づけられた複数の擬似乱数発生回路を用い、前段の前記擬似乱数発生回路が発生した第１の擬似乱数にもとづいて各擬似乱数発生回路に第１の擬似乱数を発生させ、前記複数の擬似乱数発生回路が発生した前記第１の擬似乱数により第２の擬似乱数を発生する擬似乱数発生方法において、各擬似乱数発生回路では、複数のビットから成る状態データを保持し、保持した前記状態データに応じて複数のビットから成る第１および第２のデータを発生し、前記第１および第２のデータのうちのいずれかのデータの特定のビットを、前段の前記擬似乱数発生回路が発生した前記第１の擬似乱数にもとづいて選択し前記第１の擬似乱数として出力し、前記第１および第２のデータのうちのいずれかのデータの、前記特定のビットを除いたデータを、前段の前記擬似乱数発生回路が発生した前記第１の擬似乱数にもとづいて選択し次に保持すべき前記状態データとすることを特徴とする。

【００１７】本発明の擬似乱数発生方法はまた、保持した前記状態データに応じて複数のビットから成る順序づけられた複数のデータを発生し、前記複数のデータのうちの１番目のデータは前記状態データから直接発生し、２番目以降のデータはそれぞれ１つ前のデータから発生し、前記第１のデータは前記複数のデータのうちの最後のデータを除くいずれかのデータであり、前記第２のデータは前記複数のデータのうちの最後のデータであることを特徴とする。本発明は擬似乱数発生方法また、

S_0、S_1を$0<S_0<S_1$を満たす整数として前記第１のデータは前記複数のデータのうちのS_0番目のデータであって前記第２のデータはS_1番目の前記データであり、ｉを１以上の整数としてｉ番目の前記擬似乱数発生回路が発生する前記第１の擬似乱数の系列の周期をL_iとし、ｉ番目の前記擬似乱数発生回路が発生する前記第１の擬似乱数の系列の１周期中に出現する論理”１”の数をW_iとし、任意のｉに対してL_iと$(L_{i-1}-W_{i-1})\times S_0+W_{i-1}\times S_1$とが互いに素で、２より大きい任意のｉに対して$L_i$と$L_1\times L_2\times\cdots\times L_{i-2}$とが互いに素であることを特徴とする。

【００１８】また、本発明の擬似乱数発生装置は、順序づけられた複数の擬似乱数発生回路を備え、各擬似乱数発生回路は前段の前記擬似乱数発生回路が発生した第１の擬似乱数にもとづいて第１の擬似乱数を発生し、前記複数の前記擬似乱数発生回路が発生した前記第１の擬似乱数により第２の擬似乱数を発生する擬似乱数発生装置において、各擬似乱数発生回路は、複数のビットから成る状態データを、クロック信号の各クロックパルスに同期して取り込んで保持するレジスタと、前記レジスタが保持している前記状態データに応じて複数のビットから成る第１および第２のデータをそれぞれ出力する第１および第２の関数発生回路と、前記第１および第２の関数発生回路がそれぞれ出力する前記第１および第２のデータのうちのいずれかのデータの特定のビットを、前段の前記擬似乱数発生回路が発生した前記第１の擬似乱数にもとづいて選択し前記第１の擬似乱数として出力する第１のセレクタと、前記第１および第２の関数発生回路がそれぞれ出力する前記第１および第２のデータのうちのいずれかの前記データの、前記特定のビットを除いたデータを、前段の前記擬似乱数発生回路が発生した前記第１の擬似乱数にもとづいて選択し前記レジスタに前記状態データとして供給する第２のセレクタとを備えたことを特徴とする。

【００１９】本発明の擬似乱数発生装置はまた、前記レジスタが保持している状態データに応じて複数のビットから成るデータをそれぞれ出力する順序づけられた複数の関数発生回路を含み、１番目の前記関数発生回路は前記レジスタが保持している前記状態データに直接したがって前記データを出力し、２番目以降の前記関数発生回路はそれぞれ１つ前の前記関数発生回路が出力したデータにしたがって前記データを出力し、前記第１の関数発生回路は前記複数の関数発生回路のうちの最後の関数発生回路を除くいずれかの関数発生回路であり、第２の前記関数発生回路は前記複数の関数発生回路のうちの最後の関数発生回路であることを特徴とする。本発明の擬似

乱数発生装置はまた、S_0、S_1を$0<S_0<S_1$を満たす整数として前記第１の関数発生回路は前記複数の関数発生回路のうちのS_0番目の関数発生回路であって前記第２の関数発生回路はS_1番目の関数発生回路であり、ｉを１以上の整数としてｉ番目の前記擬似乱数発生回路が発生する前記第１の擬似乱数の系列の周期をL_iとし、ｉ番目の前記擬似乱数発生回路が発生する前記第１の擬似乱数の系列の１周期中に出現する論理”１”の数をW_iとし、任意のｉに対してL_iと$(L_{i-1}-W_{i-1})\times S_0+W_{i-1}\times S_1$とが互いに素で、２より大きい任意のｉに対して$L_i$と$L_1\times L_2\times\cdots\times L_{i-2}$とが互いに素であることを特徴とする。

【００２０】本発明の擬似乱数発生方法では、擬似乱数発生回路において複数のビットから成る状態データを保持し、保持した状態データに応じて複数のビットから成る第１および第２のデータを発生する。そして、第１および第２のデータのうちのいずれかのデータの特定のビットを、前段の擬似乱数発生回路が発生した第１の擬似乱数にもとづいて選択し第１の擬似乱数として出力する。一方、第１および第２のデータのうちのいずれかのデータの、上記特定のビットを除いたデータを、前段の擬似乱数発生回路が発生した第１の擬似乱数にもとづいて選択し次に保持すべき状態データとする。

【００２１】また、本発明の擬似乱数発生装置では、擬似乱数発生回路において、レジスタは、複数のビットから成る状態データを、クロック信号の各クロックパルスに同期して取り込んで保持し、第１および第２の関数発生回路は、レジスタが保持している状態データに応じて複数のビットから成る第１および第２のデータをそれぞれ出力する。そして、第１のセレクタは、第１および第２の関数発生回路がそれぞれ出力する第１および第２のデータのうちのいずれかのデータの特定のビットを、前段の擬似乱数発生回路が発生した第１の擬似乱数にもとづいて選択し第１の擬似乱数として出力する。一方、第２のセレクタは、第１および第２の関数発生回路がそれぞれ出力する第１および第２のデータのうちのいずれかのデータの、上記特定のビットを除いたデータを、前段の擬似乱数発生回路が発生した第１の擬似乱数にもとづいて選択しレジスタに状態データとして供給する。したがって、本発明では、各擬似乱数発生回路の状態データが表す各擬似乱数発生回路の内部状態は前段が発生した擬似乱数に係わらず必ず変化し、そのためロックインの問題は発生しない。

【００２２】また、本発明の擬似乱数発生方法および擬似乱数発生装置では、第１のデータまたは第１の関数発生回路は複数のデータまたは複数の関数発生回路のうちのS_0番目のデータまたは関数発生回路であって第２のデータまたは第２の関数発生回路はS_1番目のデータまたは関数発生回路であるとし、また、ｉを１以上の整数としてｉ番目の擬似乱数発生回路が発生する第１の擬似乱数の系列の周期をL_i、ｉ番目の擬似乱数発生回路が発生する第１の擬似乱数の系列の１周期中に出現する論理”１”の数をW_iとした場合、任意のｉに対してL_iと$(L_{i-1}-W_{i-1})\times S_0+W_{i-1}\times S_1$とが互いに素で、２より大きい任意のｉに対して$L_i$と$L_1\times L_2\times\cdots\times L_{i-2}$とが互いに素であるように、$S_0$、$S_1$および$L_i$が選定される。したがって、本発明では周期が最大の擬似乱数系列を発生することができる。

【００２３】

【発明の実施の形態】次に本発明の実施の形態について図面を参照して説明する。図１は本発明による擬似乱数発生装置の一例の基本構成を示す機能ブロック図、図２は図１の擬似乱数発生装置を構成する擬似乱数発生回路を示す機能ブロック図である。以下ではこれらの図面を参照して本発明による擬似乱数発生装置の実施の形態について説明し、同時に本発明による擬似乱数発生方法の実施の形態について説明する。

【００２４】図１に示したようにこの擬似乱数発生装置１００は、複数の擬似乱数発生回路１０１を備え、擬似乱数発生回路１０１には、入力端子１０３を通じてクロック信号ＣＬＫが入力され、入力端子１０４からは制御信号Ｌが入力されている。また、入力端子１０５からは各擬似乱数発生回路１０１が最初に保持するｍビットのデータ（各擬似乱数発生回路１０１ごとに異なる）が入力される。ｉ番目（ｎを正の整数としてｉ＝１、２、．．．、ｎ）の擬似乱数発生回路１０１が発生した擬似乱数X_i（本発明に係わる第１の擬似乱数）は次段（ｉ＋１番目）の擬似乱数発生回路１０１に状態制御信号として入力される。ただし、最初の擬似乱数発生回路１０１には、論理値が一定（本実施の形態では論理”０”）の状態制御信号（X_0）が入力されている。排他的論理和回路１０２は、すべての擬似乱数発生回路１０１が発生した擬似乱数$X_{1\sim n}$の排他的論理和を計算し、計算結果をこの擬似乱数発生装置１００が発生した擬似乱数（本発明に係わる第２の擬似乱数）として出力端子１０６を通じて出力する。

【００２５】擬似乱数発生回路１０１は、後に詳しく説明するように内部状態をスキップする機能を有し、具体的には図２に示したように、レジスタ２０５、関数発生回路２０２１、２０２２、セレクタ２０３、２０６により構成されている。レジスタ２０５は、入力端子２１５からクロック信号ＣＬＫの各クロックパルスが供給されるごとに、セレクタ２０６が出力しているｍビットのデータを内部状態を表すデータ（本発明に係わる状態データ）として取り込んで保持し、同時に、保持したデータを関数発生回路２０２１に出力する。

【００２６】関数発生回路２０２１は、レジスタ２０５から供給されるｍビットのデータに対して予め決められた変換を施し、もとのデータより１ビット多いｍ＋１ビットのデータを発生し、発生したデータの各ビットのう

ちｍビットを関数発生回路２０２２とセレクタ２０６とに供給し、一方、残りの１ビット（本発明に係わる特定のビット）をセレクタ２０３に供給する。関数発生回路２０２２は関数発生回路２０２１と同様に構成され、関数発生回路２０２１から供給されるｍビットのデータに対して予め決められた変換を施して、ｍ＋１ビットのデータを発生し、発生したデータの各ビットのうちｍビットをセレクタ２０６に供給し、一方、残りの１ビットをセレクタ２０３に供給する。なお、関数発生回路２０２２は関数発生回路２０２１からのデータにもとづいて新たなデータを発生するので、結局レジスタ２０５が保持しているデータに応じて新たなデータを発生していることになる。

【００２７】セレクタ２０６は、入力端子２１４から供給される制御信号Ｌが論理”０”の時は、入力端子２１３から供給されるｍビットのデータ$ＰＩ_i$を選択して出力する。一方、入力端子２１４から供給される制御信号Ｌが論理”１”の時は、入力端子２１６から供給される前段（ｉ－１番目）の擬似乱数発生回路１０１からの擬似乱数$Ｘ_{i-1}$（状態制御信号）が論理”０”であれば関数発生回路２０２１の出力データを選択して出力し、入力端子２１６から供給される擬似乱数$Ｘ_{i-1}$が論理”１”であれば関数発生回路２０２２の出力データを選択して出力する。

【００２８】また、セレクタ２０３は、入力端子２１６から供給される擬似乱数$Ｘ_{i-1}$が論理”０”であれば、関数発生回路２０２１の出力を選択して出力し、入力端子２１６から供給される擬似乱数$Ｘ_{i-1}$が論理”１”であれば、関数発生回路２０２２の出力を選択して出力する。そして、このセレクタ２０３の出力が、ｉ番目の擬似乱数発生回路１０１が発生した擬似乱数$Ｘ_i$として出力端子２１７より出力される。

【００２９】この擬似乱数発生回路１０１では、まず最初に論理”０”の制御信号Ｌが入力され、入力端子２１３から供給されるデータ$ＰＩ_i$がセレクタ２０６を通じてレジスタ２０５に入力され、入力端子215からクロック信号ＣＬＫのクッロクパルスが入力されると、レジスタはこのデータ$ＰＩ_i$を最初の状態データとして取り込んで保持する。その後、制御信号Ｌは論理”１”に設定され、以降、セレクタ２０３、２０６は前段の擬似乱数発生回路１０１が発生した擬似乱数発生回路$Ｘ_{i-1}$の論理値にしたがって、関数発生回路２０２１、２０２２のいずれかが出力した１ビットおよびｍビットのデータを選択してそれぞれ出力端子２１７およびレジスタ２０５に出力する。

【００３０】このように、レジスタ２０５が保持したデータは、関数発生回路２０２１、２０２４で変換され、いずれかの関数発生回路２０２１、２０２４のデータがセレクタ２０６を通じてレジスタ２０５に入力される。そして、レジスタ２０５はクロック信号ＣＬＫの各クロックパルスごとに、入力されたデータを新たな状態を表すデータとして取り込み、保持する。そのため、この擬似乱数発生回路１０１では、前段の擬似乱数発生回路１０１が発生した擬似乱数$Ｘ_{i-1}$の論理値に係わらず、クロック信号ＣＬＫの各クロックパルスが入力されるごとにレジスタ２０５は必ず新たなデータを取り込んで保持し、したがって、各クロックパルスごとに必ず内部状態が変化する。そして、このような内部状態の変化に応じて擬似乱数$Ｘ_i$が出力端子２１７から出力される。

【００３１】なお、セレクタ２０６は、入力端子２１６から供給される前段の擬似乱数発生回路１０１からの擬似乱数$Ｘ_{i-1}$（状態制御信号）が論理”１”であれば関数発生回路２０２２の出力を選択して出力するので、擬似乱数$Ｘ_{i-1}$が論理”１”のときは、本来次の内部状態を表すデータとして関数発生回路２０２１が出力しているデータはスキップされ、関数発生回路２０２２の出力データがレジスタ２０５に保持される。

【００３２】次に、このように構成された擬似乱数発生装置１００の動作について説明する。図１の擬似乱数発生装置１００に擬似乱数を発生させるには次のようにする。まず、各擬似乱数発生回路１０１の内部状態を初期化するため、各擬似乱数発生回路１０１ごとに異なるｍビットのデータを入力端子１０５に供給し、そして、入力端子１０４に論理”０”の制御信号Ｌを供給して入力端子１０３からはクロック信号ＣＬＫを供給する。その結果、各擬似乱数発生回路１０１内の上記レジスタ２０５（図２）に入力端子１０５から供給したｍビットのデータがセレクタ２０６を通じてレジスタ２０５に入力され、保持される。

【００３３】次に、入力端子１０４に論理”１”の制御信号Ｌを供給し、入力端子１０３からはクロック信号ＣＬＫを供給して通常の動作状態とする。これにより、各擬似乱数発生回路１０１では、入力端子１０３から供給したクロック信号の各クロックパルスがレジスタ２０５に入力されるごとに、レジスタ２０５は、上述のようにして関数発生回路２０２１、２０２２が発生した新たな状態を表すデータをセレクタ２０６を通じて取り込み、保持する。その際、セレクタ２０６は、前段の擬似乱数発生回路１０１が発生した擬似乱数$Ｘ_{i-1}$（状態制御信号）の論理値にしたがって関数発生回路２０２１、２０２２のいずれかが発生したデータを選択してレジスタ２０５に供給する。

【００３４】そのため、各擬似乱数発生回路１０１では、前段の擬似乱数発生回路１０１が発生した擬似乱数$Ｘ_{i-1}$の論理値が論理”０”あるいは論理”１”のいずれであっても、クロック信号ＣＬＫの各クロックパルスが入力されるごとにレジスタ２０５は必ず新たなデータを取り込んで保持し、したがって、各クロックパルスごとに必ず内部状態が変化する。

【００３５】そして、各擬似乱数発生回路１０１の関数

発生回路２０２１、２０２２はこの内部状態に応じて決る１ビットのデータを発生してセレクタ２０３に出力し、セレクタ２０３は前段の擬似乱数発生回路１０１が発生した擬似乱数X_{i-1}の論理値にもとづいて関数発生回路２０２１、２０２２からの上記１ビットのデータのいずれかを選択し、出力端子２１７から擬似乱数X_iとして出力する。排他的論理和回路１０２は、すべての擬似乱数発生回路１０１が発生した擬似乱数$X_{1\sim n}$の排他的論理和を計算し、計算結果をこの擬似乱数発生装置１００が発生した擬似乱数として出力端子１０６を通じて出力する。

【００３６】このように本実施の形態の擬似乱数発生装置１００では、各擬似乱数発生回路１０１の内部状態は前段が発生した擬似乱数（状態制御信号）の論理値に係わらず必ず変化するので、ロックインの問題は発生しない。したがって、この擬似乱数発生装置１００では暗号学的に高い安全性を備えた擬似乱数を発生することができる。また、多数の擬似乱数発生回路１０１を用いなくとも安全性の高い擬似乱数を発生することができるので、装置の小型化および低コスト化を図ることが可能である。

【００３７】なお、この擬似乱数発生装置１００では各擬似乱数発生回路１０１において２つの関数発生回路を用いたが、図３に示したようにさらに多くの関数発生回路を配列することも可能である。この擬似乱数発生回路１１０では、S_0、S_1を$0<S_0<S_1$を満たす整数として、レジスタ２０５の保持データが入力される最初の関数発生回路２０２０から数えてS_0番目の関数発生回路２０２１およびS_1番目（最後）の関数発生回路２０２２の出力データ（ｍ＋１ビット）がセレクタ２０３、２０６に供給されている。

【００３８】この擬似乱数発生回路１１０でも、上述した擬似乱数発生回路１０１の場合と同様に、前段の擬似乱数発生回路が発生した擬似乱数X_{i-1}の論理値に係わらず、クロック信号ＣＬＫの各クロックパルスが入力されるごとにレジスタ２０５は必ず新たなデータを取り込んで保持し、したがって、各クロックごとに必ず内部状態が変化する。そして、このような内部状態の変化に応じて擬似乱数X_iが出力端子２１７から出力される。そのため、擬似乱数発生回路１１０を用いた場合にもロックインを起すことなく擬似乱数を発生することができる。

【００３９】ただし、擬似乱数発生回路１１０ではより多くの関数発生回路が必要であるから、装置の規模およびコストの点では不利となる。したがって、２つの関数発生回路を用いた擬似乱数発生回路１０１は、装置の小型化と、擬似乱数の暗号学的な安全性を両立できるという点では最適である。なお、擬似乱数発生回路１１０において$S_0=1$、$S_1=2$とすると擬似乱数発生回路１１０は上述した擬似乱数発生回路１０１と同一構成となる。

【００４０】本実施の形態の擬似乱数発生装置１００では、各擬似乱数発生回路１０１のレジスタ２０５が保持する内部状態を表すデータはすべてｍビットで同一であるとしたが、本発明では従来と異なり、このビット数を各擬似乱数発生回路１０１ごとに異なる値とすることも可能である。そのような構成とした場合にも、各擬似乱数発生回路１０１は上述の場合と基本的に同様に動作してそれぞれ擬似乱数を発生し、排他的論理和回路１０２が各擬似乱数発生回路１０１が発生した擬似乱数の排他的論理和を算出することで最終的な擬似乱数が得られる。そして、内部状態を表すデータのビット数を擬似乱数発生回路ごとに変えることで多様性が増し、発生される擬似乱数はより質が向上して暗号学的な安全性は一層高まる。

【００４１】さらにパラメータを次のように最適化することにより擬似乱数発生装置１００の性能を一層高めることができる。ここでは、一般化のため擬似乱数発生装置１００は上記擬似乱数発生回路１１０で構成され、また内部状態を表すデータのビット数は擬似乱数発生回路ごとに任意に設定されているものとする。そして、ｉ番目の擬似乱数発生回路１１０が発生する擬似乱数系列の周期をL_iとし、ｉ番目の擬似乱数発生回路１１０が発生する擬似乱数系列の１周期中に出現する論理”１”の数をW_iとして、任意のｉに対してL_iと$(L_{i-1}-W_{i-1})\times S_0+W_{i-1}\times S_1$とが互いに素で、２より大きい任意のｉに対して$L_i$と$L_1\times L_2\times\cdots\times L_{i-2}$とが互いに素となるように、$S_0$、$S_1$および周期$L_i$を選定する。なお、擬似乱数発生装置１００を図１のように擬似乱数発生回路１０１で構成した場合は、S_0、S_1は$S_0=1$、$S_1=1$に選定されているので、残る周期L_iを上記条件を満たすように選定することになる。S_0、S_1および周期L_iをこのように選定することで、擬似乱数発生装置１００が出力する擬似乱数系列の周期を最大にすることができる。

【００４２】このことは、次のようにして証明できる。まず、図１において、擬似乱数X_{i-1}の周期が$L_1\times L_2\times\cdots\cdots\times L_{i-1}$で、その１周期中に出現する論理”０”の数と論理”１”の数との比が$(L_{i-1}-W_{i-1}):W_{i-1}$であると仮定する。このとき、ｉ番目の擬似乱数発生回路１１０（１０１）の内部状態は、$L_1\times L_2\times\cdots\cdots\times L_{i-1}$時間の後に、ちょうど$\{(L_{i-1}-W_{i-1})\times S_0+W_{i-1}S_1\}\times L_1\times L_2\times\cdots\cdots\times L_{i-2}$クロックパルス分だけ更新される。

【００４３】ところで、上述のように、任意のｉに対してL_iと$(L_{i-1}-W_{i-1})\times S_0+W_{i-1}\times S_1$とが互いに素で、２より大きい任意のｉに対して$L_i$と$L_1\times L_2\times\cdots\times L_{i-2}$とが互いに素となるように、$S_0$、$S_1$および周期$L_i$を選定すると、擬似乱数$X_{i-1}$とｉ番目の擬似乱数発生回路１１０（１０１）の内部状態の両方が同時に

ちょうど一巡するのは、$L_1 \times L_2 \times \cdots\cdots \times L_{i-1} \times L_i$時間の後であるから、擬似乱数$X_i$の周期は$L_1 \times L_2 \times \cdots\cdots \times L_{i-1} \times L_i$で、その間にｉ番目の擬似乱数発生回路１１０（１０１）のどの内部状態も等しい回数だけスキップされている。したがって、擬似乱数X_iの１周期中に出現する論理”０”と論理”１”の数の比は$(L_{i-1} - W_{i-1}) : W_{i-1}$となる。ところで、この仮定は、ｉ＝２の場合には成り立っているから、以上の議論は、ｉ＝２から出発して、ｉ＝２、３、．．．．、ｎについてまで適用できる。従って、擬似乱数X_nの周期（すなわち擬似乱数発生装置１００が発生する擬似乱数の周期）は$L_1 \times L_2 \times \cdots\cdots \times L_n$となる。そして、この周期は、それぞれの周期が$L_i$である擬似乱数発生回路を組み合わせて得られる擬似乱数の周期の最大値に等しい。したがって、本実施の形態の擬似乱数発生装置１００では、上記条件を満たすようにS_0、S_1、および周期L_iを選定することで、擬似乱数発生装置１００が出力する擬似乱数系列の周期を最大にすることができる。

【００４４】なお、図３の擬似乱数発生回路でS_0＝０、S_1＝１と選ぶと、擬似乱数発生回路１１０は図８に示した擬似乱数発生回路と同一構成となり、その場合、擬似乱数発生回路１１０の内部状態は、$L_1 \times L_2 \times \cdots\cdots \times L_{i-1}$時間の後に、$W_{i-1} \times L_1 \times L_2 \times \cdots\cdots \times L_{i-2}$クロックパルス分だけ更新されることになるが、図７に示した従来の擬似乱数発生装置では内部状態が常に更新されるとは限らないので、ちょうど$W_{i-1} \times L_1 \times L_2 \times \cdots\cdots \times L_{i-2}$クロックパルス分だけ常に更新されるとは言えず、以上の議論は適用できない。

【００４５】なお、擬似乱数発生装置１００では排他的論理和回路１０２により、各擬似乱数発生回路１０１が発生した擬似乱数の排他的論理和を算出して擬似乱数を得ているが、各擬似乱数発生回路１０１が発生した擬似乱数に対して排他的論理和以外の演算を行って擬似乱数を発生することも可能である。ただし、排他的論理和を使うことが、擬似乱数の暗号学的な安全性と装置の小規模化を両立できるという点で最適である。

【００４６】また、排他的論理和回路１０２の代りに各擬似乱数発生回路１０１ごとに排他的論理和回路を設ける構成とすることも可能である。図４は、各擬似乱数発生回路ごとに排他的論理和回路を設けた場合の発明の実施の形態を示す機能ブロック図である。この擬似乱数発生装置１１１では、各擬似乱数発生回路１０１ごとに排他的論理和回路８０２が設けられ、ｉ番目の排他的論理和８０２の一方の入力端子にはｉ－１番目の排他的論理和回路８０２が出力する擬似乱数Y_{i-1}が入力され、もう一方の入力端子にはｉ番目の擬似乱数発生回路１０１が発生した擬似乱数X_iが入力されている。そして、ｉ－１番目の排他的論理和回路８０２からの擬似乱数Y_{i-1}が状態制御信号としてｉ番目の擬似乱数発生回路１０１に供給されている。また、最後の排他的論理和回路８０２が算出した擬似乱数Y_nがこの擬似乱数発生装置１１１が発生した擬似乱数として出力端子１０６より出力されている。

【００４７】このような構成においても擬似乱数X_iと擬似乱数Y_iとの性質は等しいので、擬似乱数発生装置１１１は擬似乱数発生装置１００と同様に動作し、したがって擬似乱数発生装置１００と同様の効果が得られる。そして、この擬似乱数発生装置１１１では、擬似乱数発生回路１０１と排他的論理和８０２とを１つの集積回路に搭載することができ、それらをカスケード接続することによって所望の安全性を持つ擬似乱数発生装置を簡単に構成できる。

【００４８】図１の擬似乱数発生装置１００を構成する擬似乱数発生回路１０１は、図８に示した従来の擬似乱数発生回路において、関数発生回路を複数にして上述のような内部状態のスキップ機能を持たせたものである。したがって、図９に示した非線形フィードバック・シフトレジスタでも、この非線形フィードバック・シフトレジスタの基本構成は図８の擬似乱数発生回路と同じであるから、同様にして容易にスキップ機能を持たせ、図１の擬似乱数発生装置１００において、擬似乱数発生回路１０１の代りに用いることができる。そして、図８の非線形フィードバック・シフトレジスタにスキップ機能を持たせて利用した場合には、関数発生回路の構成が簡素となるので装置の小型化に有効である。

【００４９】また、図９に示したＬＦＳＲでも同様にして容易に内部状態のスキップ機能を持たせることができ、擬似乱数発生回路１０１の代りに用いることができる。この場合にも関数発生回路の構成が簡素となるので装置の小型化に有効である。

【００５０】なお、図２に示した擬似乱数発生回路１０１において、セレクタ２０６に供給されるｍビットのデータ、したがってまたレジスタ２０５に供給されるｍビットのデータはシリアルデータおよびパラレルデータのいずれであってもかまわない。そして、内部状態を表すデータのビット数が擬似乱数発生回路１０１ごとに異なる場合、１～ｎ（ｎは２以上の整数）の各擬似乱数発生回路１０１に対して最初にそれぞれm_1、m_2、……、m_nビットのデータを供給するとき、これらのデータを$m_1 + m_2 + \cdots\cdots + m_n$ビットのビット列として入力端子２１３に供給し、各擬似乱数発生回路１０のレジスタ２０５には対応するビット列部分をそれぞれ保持させるようにすることも可能である。

【００５１】次に本発明の第２の実施の形態について説明する。図５は、第２の実施の形態の擬似乱数発生装置の基本構成を示す機能ブロック図、図６は図５の擬似乱数発生装置を構成する擬似乱数発生回路を示す機能ブロック図である。図中、図１、図２と同一の要素には同一の符号が付されており、それらに関する詳しい説明はここでは省略する。

【００５２】この擬似乱数発生装置１１２が、擬似乱数発生装置１００と機能的に異なるのは複数ビットのデータとして擬似乱数を発生する点であり、一方、構成の点では、擬似乱数発生回路６０１の構成が異なり、また関数発生回路６０３が追加されている点で異なっている。図５に示したようにこの擬似乱数発生装置１１２は、多値の擬似乱数を発生する複数の擬似乱数発生回路６０１を備え、擬似乱数発生回路６０１には、入力端子１０３を通じてクロック信号ＣＬＫが入力され、入力端子１０４からは制御信号Ｌが入力されている。また、入力端子１０５からは擬似乱数発生回路６０１が最初に保持するｍビットのデータが入力される。

【００５３】ｉ番目（ｎを正の整数としてｉ＝１、２、．．．、ｎ）の擬似乱数発生回路６０１が発生した擬似乱数X_i（ｋを２以上の整数としてｋビットのデータ）は、各擬似乱数発生回路６０１ごとに設けられた関数発生回路６０３に入力され、関数発生回路６０３はこの擬似乱数X_iに予め決められた変換を施して１ビットのデータとし、擬似乱数Ｚｉ（状態制御信号）として次段（ｉ＋１番目）の擬似乱数発生回路６０１に出力する。ただし、最初の擬似乱数発生回路６０１には、論理値が一定（本実施の形態では論理”０”）の状態制御信号（Z_0）が入力されている。排他的論理和回路６０２は、すべての擬似乱数発生回路６０１が発生した擬似乱数$X_{1\sim n}$のｋビットのデータとしての排他的論理和を計算し、計算結果をこの擬似乱数発生装置１１２が発生したｋビットの擬似乱数として出力端子１０６を通じて出力する。

【００５４】ｉ番目の擬似乱数発生回路６０１は図６に示したように、レジスタ２０５、関数７０２１、７０２２、セレクタ７０３、２０６により構成されている。レジスタ２０５は、入力端子２１５からクロック信号ＣＬＫの１つのクロックパルスが供給されるごとに、セレクタ２０６が出力しているｍビットのデータを内部状態を表すデータ（本発明に係わる状態データ）として保持し、同時に、保持したデータを関数発生回路７０２１に出力する。

【００５５】関数発生回路７０２１は、レジスタ２０５から供給されるｍビットのデータに対して予め決められた変換を施し、もとのデータよりｋビット多いｍ＋ｋビットのデータを発生し、発生したデータの各ビットのうちｍビットを関数発生回路７０２２とセレクタ２０６とに供給し、一方、残りのｋビット（本発明に係わる特定のビット）をセレクタ７０３に供給する。関数発生回路７０２２は関数発生回路７０２１と同様に構成され、関数発生回路７０２１から供給されるｍビットのデータに対して予め決められた変換を施して、ｍ＋ｋビットのデータを発生し、発生したデータの各ビットのうちｍビットをセレクタ２０６に供給し、一方、残りのｋビットをセレクタ７０３に供給する。なお、関数発生回路７０２２は関数発生回路７０２１からのデータにもとづいて新たなデータを発生するので、結局レジスタ２０５が保持しているデータに応じて新たなデータを発生していることになる。

【００５６】セレクタ７０３は、入力端子２１６から供給される前段からの擬似乱数Z_{i-1}（状態制御信号）が論理”０”であれば、関数発生回路７０２１の出力を選択して出力し、入力端子２１６から供給される状態制御信号Z_{i-1}が論理”１”であれば、関数発生回路７０２２の出力を選択して出力する。そして、このセレクタ７０３の出力が、擬似乱数発生回路６０１が発生したｋビットの擬似乱数X_iとして出力端子７１７より出力される。

【００５７】この擬似乱数発生回路６０１でも、セレクタ２０６は、入力端子２１６から供給される前段の擬似乱数発生回路６０１からの状態制御信号Z_{i-1}が論理”１”であれば関数発生回路７０２２の出力を選択して出力するので、状態制御信号Z_{i-1}が論理”１”のときは、本来次の内部状態を表すデータとして関数発生回路７０２１が出力しているデータはスキップされ、関数発生回路７０２２の出力データがレジスタ２０５に保持される。

【００５８】この擬似乱数発生回路６０１では、まず最初に論理”０”の制御信号Ｌが入力され、入力端子２１３から供給されるデータPI_iがセレクタ２０６を通じてレジスタ２０５に入力され、入力端子215からクロック信号ＣＬＫのクロックパルスが入力されると、レジスタはこのデータPI_iを最初の状態データとして取り込んで保持する。その後、制御信号Ｌは論理”１”に設定され、以降、セレクタ７０３、２０６は前段の関数発生回路６０３が発生した擬似乱数Z_{i-1}の論理値にしたがって、関数発生回路７０２１、７０２２のいずれかが出力したｋビットおよびｍビットのデータを選択してそれぞれ出力端子７１７およびレジスタ２０５に出力する。

【００５９】このように、レジスタ２０５が保持したデータは、関数発生回路７０２１、７０２２で変換され、いずれかの関数発生回路７０２１、７０２２のデータがセレクタ２０６を通じてレジスタ２０５に入力される。そして、レジスタ２０５はクロック信号ＣＬＫの各クロックパルスごとに、入力されたデータを新たな状態を表すデータとして取り込み、保持する。

【００６０】そのため、この擬似乱数発生回路６０１では、前段の関数発生回路６０３が発生した擬似乱数Z_{i-1}の論理値に係わらず、クロック信号ＣＬＫの各クロックパルスが入力されるごとにレジスタ２０５は必ず新たなデータを取り込んで保持し、したがって、各クロックごとに必ず内部状態が変化する。そして、このような内部状態の変化に応じてｋビットの擬似乱数X_iが出力端子２１７から出力される。

【００６１】次に、このように構成された擬似乱数発生

装置１１２の動作について説明する。図５の擬似乱数発生装置１１２に擬似乱数を発生させるには次のようにする。まず、各擬似乱数発生回路６０１の内部状態を初期化するためのｍビットのデータ（擬似乱数発生回路６０１ごとに異なる）を入力端子１０５に供給し、そして、入力端子１０４に論理”０”の制御信号Ｌを供給して入力端子１０３からはクロック信号ＣＬＫを入力する。その結果、各擬似乱数発生回路６０１内の上記レジスタ２０５（図６）に入力端子１０５から供給したｍビットのデータがセレクタ２０６を通じてレジスタ２０５に入力され、保持される。

【００６２】次に、入力端子１０４に論理”１”の制御信号Ｌを供給し、入力端子１０３からはクロック信号ＣＬＫを供給して通常の動作状態とする。これにより、各擬似乱数発生回路６０１では、入力端子１０３から供給したクロック信号の各クロックパルスがレジスタ２０５に入力されるごとに、レジスタ２０５は、上述のようにして関数発生回路７０２１、７０２２が発生した新たな状態を表すデータをセレクタ２０６を通じて取り込み、保持する。その際、セレクタ２０６は、前段の擬似乱数発生回路６０１が発生した擬似乱数X_{i-1}を関数発生回路６０３が変換して発生した擬似乱数Z_{i-1}（状態制御信号）の論理値にしたがって関数発生回路７０２１、７０２２のいずれかが発生したデータを選択してレジスタ２０５に供給する。

【００６３】そのため、各擬似乱数発生回路６０１では、前段の擬似乱数発生回路６０１に対応する関数発生回路６０３が発生した擬似乱数Z_{i-1}（状態制御信号）の論理値が論理”０”あるいは論理”１”のいずれであっても、クロック信号ＣＬＫの各クロックパルスが入力されるごとにレジスタ２０５は必ず新たなデータを取り込んで保持し、したがって、各クロックごとに必ず内部状態が変化する。

【００６４】そして、各擬似乱数発生回路６０１の関数発生回路７０２１、７０２２はこの内部状態に応じて決るｋビットのデータを発生してセレクタ７０３に出力し、セレクタ７０３は前段の擬似乱数発生回路６０１に対応する関数発生回路６０３が発生した擬似乱数Z_{i-1}（状態制御信号）の論理値にもとづいて関数発生回路７０２１、７０２２からの上記ｋビットのデータのいずれかを選択し、出力端子７１７からｋビットの擬似乱数X_iとして出力する。排他的論理和回路６０２は、すべての擬似乱数発生回路６０１が発生した擬似乱数$X_{1\sim n}$の排他的論理和を計算し、計算結果をｋビットの擬似乱数として出力端子６０６を通じて出力する。

【００６５】したがってこの擬似乱数発生装置１１２でも、各擬似乱数発生回路６０１の内部状態は前段が発生した擬似乱数にもとづく状態制御信号の論理値に係わらず必ず変化するので、ロックインの問題は発生しない。そのため、擬似乱数発生装置１１２では暗号学的に高い安全性を備えた擬似乱数を発生することができる。また、多数の擬似乱数発生回路６０１を用いなくとも安全性の高い擬似乱数を発生することができるので、装置の小型化および低コスト化を図ることが可能である。なお、この擬似乱数発生装置１１２では各擬似乱数発生回路６０１において２つの関数発生回路を用いたが、擬似乱数発生装置１００の場合と同様、擬似乱数発生回路１１０（図３）のようにさらに多くの関数発生回路を配列することも可能である。ただし、そのような構成ではより多くの関数発生回路が必要であるから、装置の規模およびコストの点では不利となる。したがって、２つの関数発生回路を用いた擬似乱数発生回路６０１は、装置の小型化と、擬似乱数の暗号学的な安全性を両立できるという点では最適である。

【００６６】また、この擬似乱数発生装置１１２では、各擬似乱数発生回路６０１のレジスタ２０５が保持する内部状態を表すデータはすべてｍビットで同一であるとしたが、擬似乱数発生装置１００の場合と同様に、このビット数を各擬似乱数発生回路６０１ごとに異なる値とすることも可能である。そのような構成とした場合にも、各擬似乱数発生回路６０１は上述の場合と基本的に同様に動作してそれぞれ擬似乱数を発生し、排他的論理和回路６０２が各擬似乱数発生回路６０１が発生した擬似乱数の排他的論理和を算出することで擬似乱数が得られる。そして、内部状態を表すデータのビット数を擬似乱数発生回路ごとに変えることで多様性が増し、発生される擬似乱数はより質が向上して暗号学的な安全性は一層高まる。

【００６７】さらに、この擬似乱数発生装置１１２においてもパラメータを最適化することにより性能を一層高めることができる。すなわち、ｉ番目の擬似乱数発生回路６０１が発生する擬似乱数系列の周期をL_iとし、ｉ番目の関数発生回路６０３が出力する状態制御信号Z_i（擬似乱数系列）の１周期中に出現する論理”１”の数をW_iとして、任意のｉに対してL_iと$(L_{i-1}-W_{i-1})\times S_0+W_{i-1}\times S_1$とが互いに素で、２より大きい任意のｉに対して$L_i$と$L_1\times L_2\times\cdots\times L_{i-2}$とが互いに素となるように、$S_0$、$S_1$および周期$L_i$を選定する。

【００６８】なお、一般化のため擬似乱数発生回路６０１において内部状態を表すデータのビット数は擬似乱数発生回路６０１ごとに任意に設定されているものとする。また、S_0、S_1は、擬似乱数発生回路１１０の場合と同様、擬似乱数発生回路６０１において関数発生回路をさらに多数配列した場合に、何番目の関数発生回路からセレクタ２０６にデータが供給されているかを表す数であり、S_0番目とS_1番目の関数発生回路からセレクタ２０６にデータが供給され、S_1番目の関数発生回路が最後の関数発生回路である。S_0、S_1および周期L_iを上記条件を満たすように選定することで、擬似乱数発生装置１１２が出力する擬似乱数系列の周期を最大にする

ことができる。このことは、擬似乱数発生装置１００の場合と同様にして証明できるので、ここではその証明は省略する。なお、擬似乱数発生装置１１２ではS_0＝１、S_1＝２であるから、擬似乱数発生装置１１２の場合は上記条件を満たすように周期L_iを選定することになる。

【００６９】擬似乱数発生装置１１２では排他的論理和回路６０２により、各擬似乱数発生回路６０１が発生した擬似乱数の排他的論理和を算出して擬似乱数を得ているが、各擬似乱数発生回路６０１が発生した擬似乱数に対して排他的論理和以外の演算を行って擬似乱数を発生することも可能である。ただし、排他的論理和を使うことが、擬似乱数の暗号学的な安全性と装置の小規模化を両立できるという点で最適である。また、擬似乱数発生装置１１１（図４）のように、排他的論理和回路６０２の代りに各擬似乱数発生回路６０１ごとに排他的論理和回路を設ける構成とすることも可能である。

【００７０】

【発明の効果】以上説明したように本発明の擬似乱数発生方法では、擬似乱数発生回路において複数のビットから成る状態データを保持し、保持した状態データに応じて複数のビットから成る第１および第２のデータを発生する。そして、第１および第２のデータのうちのいずれかのデータの特定のビットを、前段の擬似乱数発生回路が発生した第１の擬似乱数にもとづいて選択し第１の擬似乱数として出力する。一方、第１および第２のデータのうちのいずれかのデータの、上記特定のビットを除いたデータを、前段の擬似乱数発生回路が発生した第１の擬似乱数にもとづいて選択し次に保持すべき状態データとする。

【００７１】また、本発明の擬似乱数発生装置では、擬似乱数発生回路において、レジスタは、複数のビットから成る状態データを、クロック信号の各クロックパルスに同期して取り込んで保持し、第１および第２の関数発生回路は、レジスタが保持している状態データに応じて複数のビットから成る第１および第２のデータをそれぞれ出力する。そして、第１のセレクタは、第１および第２の関数発生回路がそれぞれ出力する第１および第２のデータのうちのいずれかのデータの特定のビットを、前段の擬似乱数発生回路が発生した第１の擬似乱数にもとづいて選択し第１の擬似乱数として出力する。一方、第２のセレクタは、第１および第２の関数発生回路がそれぞれ出力する第１および第２のデータのうちのいずれかのデータの、上記特定のビットを除いたデータを、前段の擬似乱数発生回路が発生した第１の擬似乱数にもとづいて選択しレジスタに状態データとして供給する。

【００７２】したがって、本発明では、各擬似乱数発生回路の状態データが表す各擬似乱数発生回路の内部状態は前段が発生した擬似乱数に係わらず必ず変化し；そのためロックインの問題は発生しない。その結果、本発明では暗号学的に高い安全性を備えた擬似乱数を発生できる。また、ロックインの問題がないので多数の擬似乱数発生回路を用いなくとも安全性の高い擬似乱数を発生することができ、装置の小型化および低コスト化を図ることが可能である。そして、本発明では状態データのビット数を擬似乱数発生回路ごとに変えることが可能であるから、多様性を増大させて、発生される擬似乱数の質を一層向上させ、暗号学的な安全性を一層高めることができる。さらに、擬似乱数を複数のビットから成るデータとして発生する多値の擬似乱数発生回路を用いることができるので、より利用範囲を拡大することができる。

【００７３】また、本発明の擬似乱数発生方法および擬似乱数発生装置では、第１のデータまたは第１の関数発生回路は複数のデータまたは複数の関数発生回路のうちのS_0番目のデータまたは関数発生回路であって第２のデータまたは第２の関数発生回路はS_1番目のデータまたは関数発生回路であるとし、また、ｉを１以上の整数としてｉ番目の擬似乱数発生回路が発生する第１の擬似乱数の系列の周期をL_i、ｉ番目の擬似乱数発生回路が発生する第１の擬似乱数の系列の１周期中に出現する論理”１”の数をW_iとした場合、任意のｉに対してL_iと$(L_{i-1}-W_{i-1})\times S_0+W_{i-1}\times S_1$とが互いに素で、２より大きい任意のｉに対して$L_i$と$L_1\times L_2\times\cdots\times L_{i-2}$とが互いに素であるように、$S_0$、$S_1$および$L_i$が選定される。したがって、本発明では周期が最大の擬似乱数系列を発生することができる。

【図面の簡単な説明】

【図１】本発明による擬似乱数発生装置の一例の基本構成を示す機能ブロック図である。

【図２】図１の擬似乱数発生装置を構成する擬似乱数発生回路を示す機能ブロック図である。

【図３】より多くの関数発生回路を用いた擬似乱数発生回路を示す機能ブロック図である。

【図４】各擬似乱数発生回路ごとに排他的論理和回路を設けた場合の発明の実施の形態を示す機能ブロック図である。

【図５】第２の実施の形態の擬似乱数発生装置の基本構成を示す機能ブロック図である。

【図６】図５の擬似乱数発生装置を構成する擬似乱数発生回路を示す機能ブロック図である。

【図７】線形フィードバック・シフトレジスタ（ＬＦＳＲ）をカスケード接続した従来の擬似乱数発生装置の基本構成を示す機能ブロック図である。

【図８】従来の基本的な構成の擬似乱数発生回路の一例を示す機能ブロック図である。

【図９】非線形フィードバック・シフトレジスタと呼ばれる従来の擬似乱数発生回路の基本構成を示す機能ブロック図である。

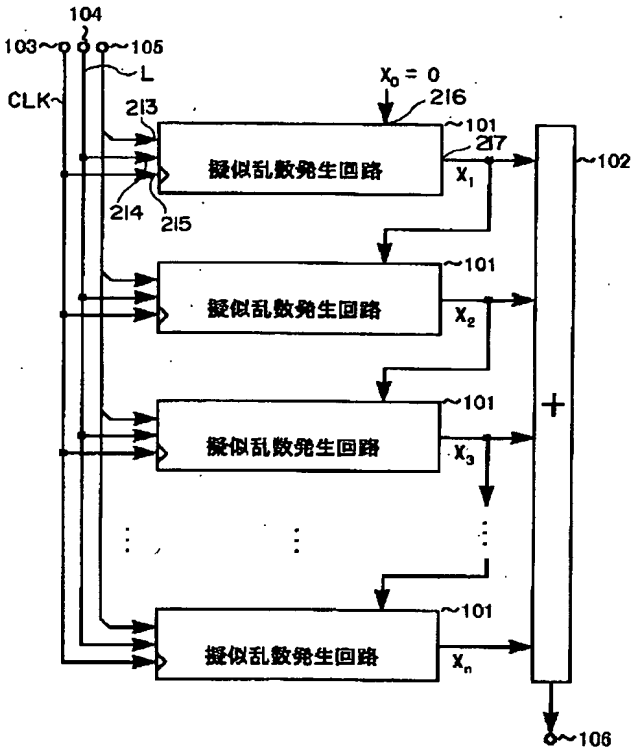
【図１０】図７の擬似乱数発生装置を構成する線形フィードバック・シフトレジスタの基本構成を示す機能ブロ

ック図である。

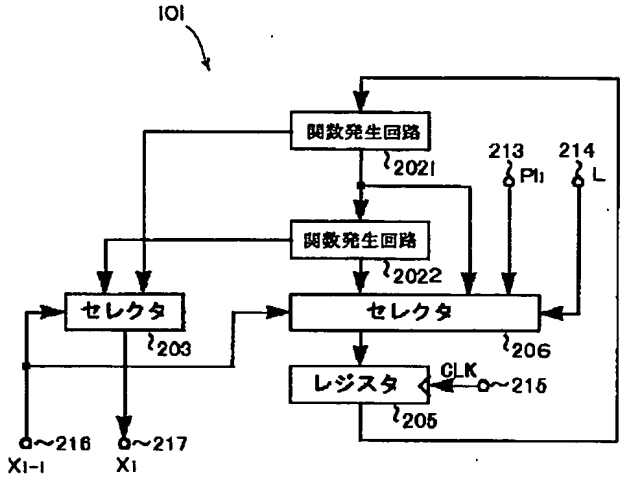
【符号の説明】

１００、１１１、１１２……擬似乱数発生装置、１０１、１１０、６０１……擬似乱数発生回路、１０２、６０２、８０２……排他的論理和回路、２０５……レジスタ、２０３、２０６、７０３……セレクタ、６０３、２０２１、２０２０、２０２２、７０２１、７０２２……関数発生回路。

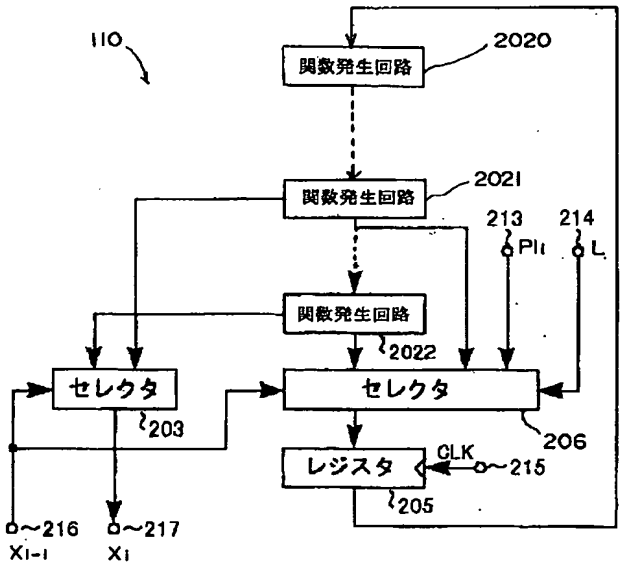
【図１】



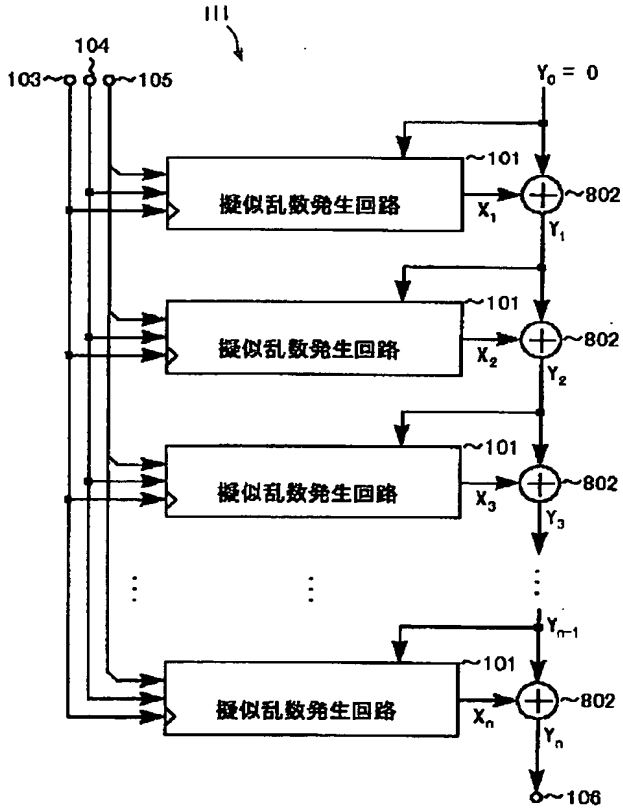
【図２】



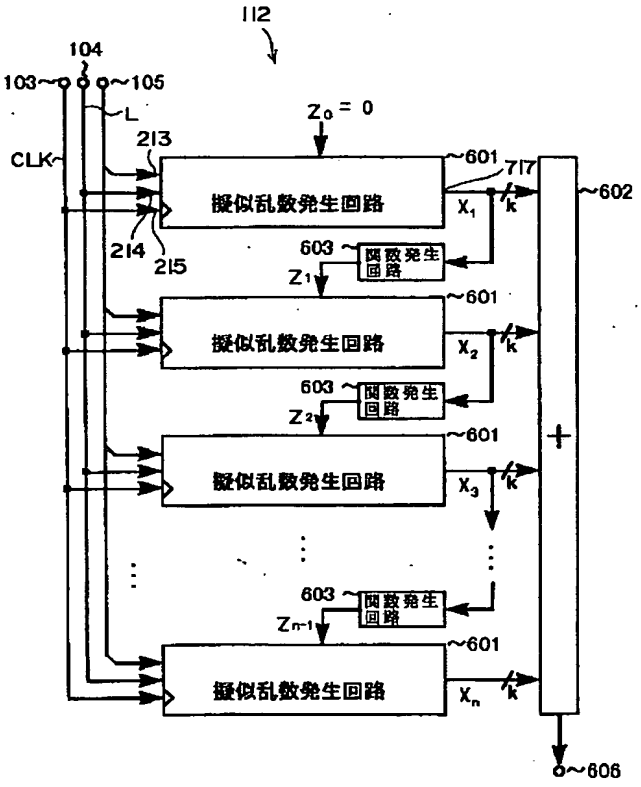
【図３】



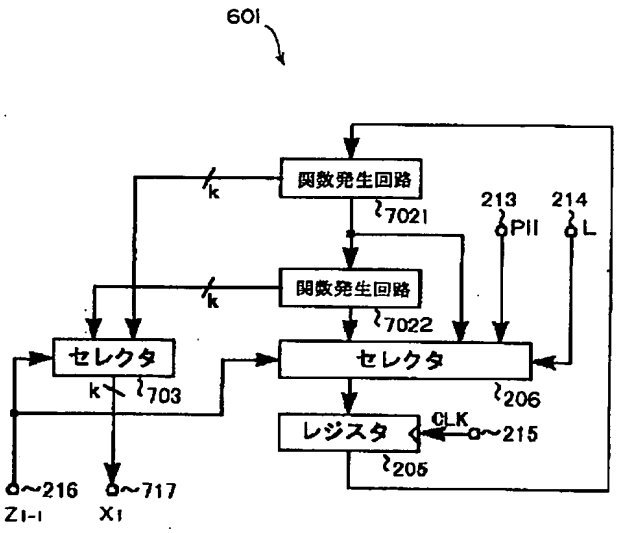
【図４】



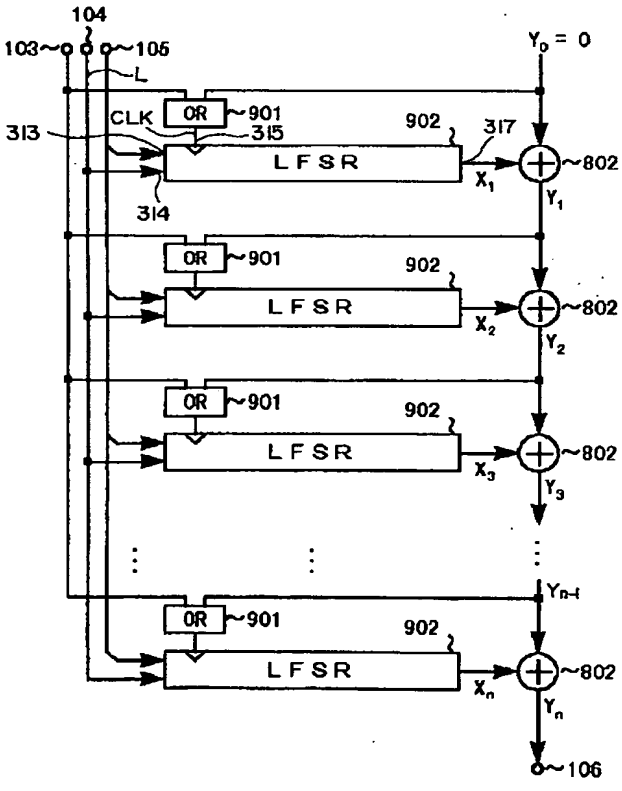
【図５】


112
104
103
105
L
CLK
213
214
215
$Z_0 = 0$
601
717
602
擬似乱数発生回路
X_1
k
603
関数発生回路
Z_1
X_2
Z_2
X_3
Z_{n-1}
X_n
606

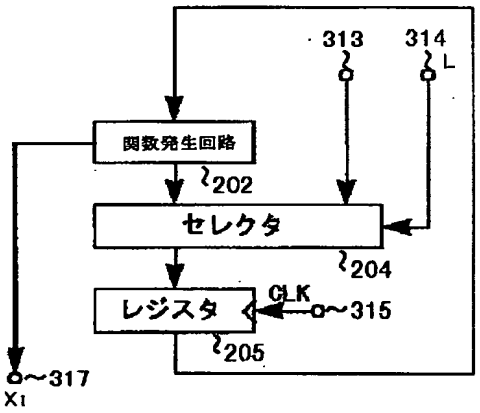
【図６】


601
関数発生回路
7021
7022
213
PII
214
L
k
セレクタ
703
206
レジスタ
CLK
215
205
216
Z_{I-1}
717
X_I

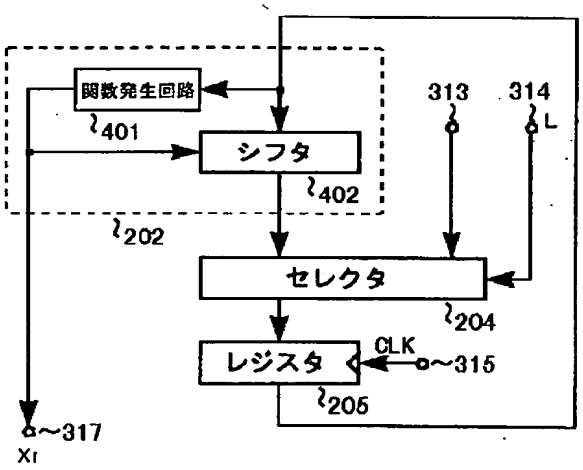
【図７】


104
103
105
L
$Y_0 = 0$
CLK
313
OR
901
315
902
317
LFSR
X_1
802
Y_1
314
X_2
Y_2
X_3
Y_3
Y_{n-1}
X_n
Y_n
106

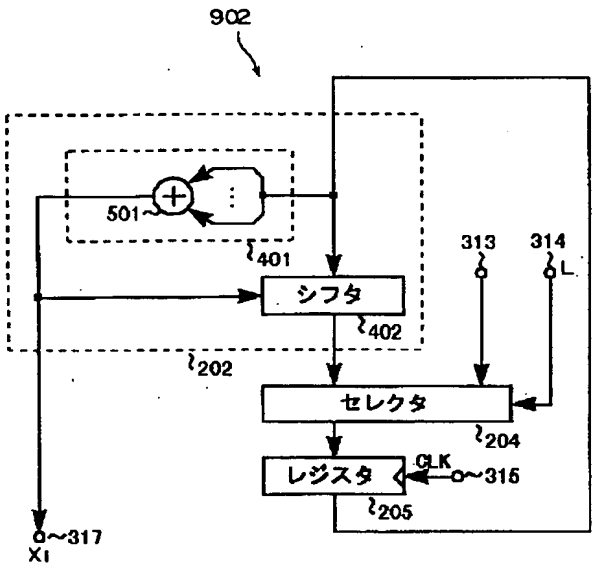
【図８】


313
314
L
関数発生回路
202
セレクタ
204
レジスタ
CLK
315
205
317
X_I

【図９】


関数発生回路
401
シフタ
402
202
313
314
L
セレクタ
204
レジスタ
CLK
315
205
317
X_I

【図１０】


902
501
401
313
314
L
シフタ
402
202
セレクタ
204
CLK
315
レジスタ
205
317
XI